



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/720,353	12/21/2000	Michael Nolte	6400-11WOUS	1134

7590 05/06/2004
McCormick Paulding & Huber
City Place II
185 Asylum Street
Hartford, CT 06103-4102

EXAMINER

POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 05/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/720,353

Applicant(s)

NOLTE, MICHAEL

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on April 29, 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on _____ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- 1) ☐ Certified copies of the priority documents have been received.
 - 2) ☐ Certified copies of the priority documents have been received in Application No. _____.
 - 3) ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10 are pending and have been examined.

Information Disclosure Statement

2. The information disclosure statement filed 12/21/00 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because "A Beutelspacher et al., "Chipkarten als Sicherheitswerkzeug" does not contain a publication date. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR §1.97(e). See MPEP § 609 ¶ C(1).

Priority

3. Foreign priority has been claimed in this application.
Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Germany on 4/30/1999. It is noted, however, that applicant has not filed a certified copy of the German application as required by 35 U.S.C. 119(b).

The effective priority date for the subject matter in the pending claims in this application once the paper has been received will be 4/30/1999.

Specification

4. For the purposes of consistency, the specification under the brief description of drawings should refer to "Fig.1".

Abstract

5. "The receiver" in line 2 and "the sender" in lines 5-6 are not defined.
"The signature *on* the message" statement in the last sentence is understood as "the signature *of* the message".

Claim Objections

6. Claims 1 - 10 are objected to because of the following informalities:

Claim 7 line 3: the statement "possibly together" does not allow the examiner to determine whether the applicant means that signing keys are sent by themselves or with the associated sequence numbers. The examiner considers the statement as if it read "by themselves or" indicating that the sequence key can be sent from the control center to the sender by themselves or together with the associated sequence numbers.

The application *claims 1-10* use numbers in order to clarify the invention.

However, in *Claim 1* lines 17 and 29, *claim 2* last sentence, and *claim 9* line 6 the

referring numbers introduce some confusion where within brackets several numbers are provided even though the preceding text refers to a single concept. Due to the possible confusion the examiner objects to the use of the reference numbers within the claims as they are provided. See MPEP 608.01m and 2173.05(s).

Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1 -10 are rejected as follows:

Claim 1 recites the limitation "the one check key" in line 23. There is insufficient antecedent basis for this limitation in the claim.

Also, it is unclear how the receiver is to determine the sequence number since there is no previous step that requires the sequence number to be received.

Claim 1 recites "a receiver" in lines 5-6. It is unclear whether this introduces a new receiver or if it refers to the earlier introduced (lines 4-5) receiver. For further consideration the examiner will consider that the application refers to the same entity as though the line 5-6 was written "the receiver".

Claim 1 line 26 does not clearly define "this". As a result the metes and bounds of the claim cannot be determined.

Claims 3 and 4 are unclear. It is unclear what “the number of signing and check keys” the application refers to. Also, the application indicates that “signing keys” are being used only in the control center and “check keys” are used by a receiver.

For further consideration the examiner will consider the meaning of the *claim 3* as follows: ***“The method as claimed in claim 1, wherein the sequence numbers are used to produce signing keys used in the control center and corresponding check keys used by the receiver”***. The *claim 4* will be considered as follows: ***“The method as claimed in claim 1, wherein the sequence numbers are used to produce signing keys used in the control center and corresponding check keys used by the receiver. The sequence number is transmitted via the data set to the receiver”***.

Claim 9 lines 4-5: the statement “a control center and the receiver have a first and second memory” is not clear as to whether both the control center and the receiver have both a first and second memory or the control center has a first memory and the receiver has the second memory. In the light of the lines 9 and 32 the examiner will consider the statement meaning as follows: “a control center has a first memory and the receiver has a second memory”.

Claim 9 recites “the protected memory” in line 9. The protected memory has not been defined. There is insufficient antecedent basis for this limitation in the claim. The examiner considers that the reference is made to the control center memory.

Claim 10 recites "The device as claimed in claim 9, wherein a generator using a deterministic method produces one or more sequence numbers corresponding to the number of checks". It is unclear what the sentence means. It is unclear what "number of checks" the application refers to and how the sequence numbers correspond to them.

Claims 2 and 4-8 are rejected by virtue of their dependence.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

9. Claims 1-7 are rejected under 35 U.S.C. 102(a) as being anticipated by *Deo et al.* (U.S. Patent No. 6,496,928).

Re claim 1: Deo et al. teaches a method for encrypting a message by a sender, and for decrypting the message by a receiver, wherein a control center and a receiver have a secret, common main key (*current broadcast key, Deo et al., col. 26, lines 7-8*) having the following feature:

the control center

- produces a sequence number (*message specific data*) (*Deo et al., fig. 9A and col. 26, lines 7-23*)

- from this and using the main key produces a signing key (*message specific key*) by means of one-time encryption (*HMAC*), and (*Deo et al., fig. 9A and col. 26, lines 7-23*)
- provides the sender with the signing key; (*Deo et al., fig. 9A and col. 26, lines 7-23*)

the sender

- uses the signing key to encrypt the message and (*Deo et al., fig. 9B and col. 26, lines 7-23*)
- sends to the receiver the encrypted message (*Deo et al., fig. 9B and col. 26, lines 7-23*)

the receiver

- determines the sequence number(*Deo et al., col. 28, lines 1-4*)
- forms the one check key using the one-time encryption and the main key and (*Deo et al., col. 28, lines 1-4*)
- uses this to decrypt the message. (*Deo et al., col. 28, lines 1-24*)

Re claim 2: The method as claimed in claim 1, wherein the sequence number is transmitted together with the signing key from the control center to the sender, and is transmitted from the sender via the data set to the receiver (*Deo et al., fig. 9A, 9B and 9C, col. 26 lines 30-32 and 42-43*)

Re claim 3: The method as claimed in claim 1, wherein the sequence number is produced by a generator in synchronism with the number of signing and check

keys used in the control center and in the receiver (*Deo et al.*, col. 24, lines 37-41, col. 26, lines 7-23, col. 28, lines 1-4).

The method as claimed in claim 1, wherein the sequence number is produced by a generator in synchronism with the number of signing and check keys used in the control center and in the sender, and is transmitted via the data set to the receiver. (*Deo et al.*, col. 24, lines 37-41, col. 26, lines 7-23 and 43-44, col. 28, lines 1-4).

Re claim 5: The method as claimed in claim 1, wherein the sequence number is produced by a pseudo-random number generator (*Deo et al.*, col. 24, lines 39-40).

Re claim 6: The method as claimed in claim 1, wherein the encryption of the sequence number by means of the main key is used as the one-time encryption (*Deo et al.*, col. 26, lines 7-23).

Re claim 7: The method as claimed in claim 1, wherein the control center produces a number of signing keys in advance, and transmits them to the sender, possibly together with the associated sequence numbers (*Deo et al.*, col. 24, lines 37-41, col. 26, lines 7-23 and 43-44, col. 28, lines 1-4).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2134

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Deo et al.*, (U.S. Patent No. 6,496,928) as applied to claim 8 above, in view of *Horstmann* (U.S. Patent No 6009401).

Re claim 8: Deo et al. states claim 1 as outlined above. *Deo et al.* does not teach a method wherein the receiver maintains a list of already used sequence numbers, and rejects already used sequence numbers. However, it is well known in the art that replay attacks are used to break communicating systems security. *Horstmann* employs a list to avoid reusing objects in order to prevent replay attacks (*Horstmann*, col.5 lines 21-27). Thus, it would be obvious to an ordinary person skilled in the arts to implement the teaching into the method as claimed in claim 1, so that the receiver maintains a list of already used sequence numbers, and rejects already used sequence numbers.

Allowable Subject Matter

Claims 9 and 10 are being rejected based on second paragraph of 35 U.S.C. 112, but would be allowable if the rejection was appropriately addressed.

Conclusion

No claim is allowed.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (703) 305-0719. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-9000.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:


(703) 746-7239 (for formal communications intended for entry)

Or:

(703) 746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered response should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free)


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100